Common Virus Removal 2015

Steps to easily identify and remove most common infections

By Charles Hornat

Contents

Overview

Often times I am asked, what's the best way to remove infections from a computer? How do I know if I am infected? Or other questions along this topic. This paper covers some things to consider, as well as areas to look at on your computer, and tactics in which to remove possible infections. This paper is geared towards windows 7 and windows 8.

Disclaimer

Performing certain actions in the paper may have irreversible and dire consequences on your computer. This is more geared towards someone who has a backup of their data, and access to someone or the knowledge to rebuild their computer if all else fails. It also should be noted that this paper does not apply to every infection out there, just the common infections that we see in our client networks/computers.

Please note that sophisticated attacks or infections require more sophisticated approach. This is more of a layman's way of identifying infections.

Who am I

Someone who owns and operates a consulting company with clients in the US and Mexico. These clients range from 1-200 person organizations. These clients get infected with the latest and greatest from time to time requiring a systematic approach to cleaning and recovering.

I have over 20 years of experience researching and protecting networks and computers around the world. These are my notes.

Am I infected?

Infections today have more purpose than just creating havoc on your computer or network. Today they attempt to steal passwords, banking information or other confidential information. Therefore, they are designed to hide from an average user and stay hidden in order to continue to capture your data.

Some common ways to tell if you are infected is if:

- your web browser is constantly redirecting you to a site you don't want to go to,
- you run out of disk space or hard drive fills up,
- your computer becomes very slow,
- You're notified that your data, email and password to a site(s) has been compromised
- You are prompted by a program you are not familiar with that you are infected and need to click a button in order to clean it up,
- You are notified that your Flash/Java/whatever is out of date and you need to update.

If you experience any of the above, it's time to investigate.

Pre-step

There are a few suggestions that I make for anyone working with an infected machine. Here is a quick list of guidelines.

1. Disconnect the system from the Internet until you understand what you are working with. Spend time researching and understanding what has been compromised, if anything. Additionally, if you are dealing with a network encrypting program like Cryptoware, this action is the most critical to stop it from doing any harm to network files.
2. In windows explorer, be sure to enable the option to view all hidden files, and display the extensions of files.
3. Any tools you decide to run, download on a clean system and transfer via a USB or CD to the infected system. Do not download from the Internet directly on to the infected system.

Step 1: Identify the startup of the infection

Infections need to start up somehow. There are a few common ways, and we will look at each process in detail. The startup procedures we will look at include:

- Startup Folder
- Registry
- Task Scheduler

Startup Folder

The simplest approach, and possibly the least sophisticated is to put the malicious software in your startup folder. Every time your computer starts up, it looks at this folder and runs any programs in the folder. There are two startup folders on most Windows 7 and 8 computers. The first is for a specific user, most likely the user you are logged in as, and is located at:

C:\users\%username%\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup

The second folder is for all users. No matter who logs in to the computer, this folder is checked and any programs in this folder are run at the time of logging in. The folder is located at:

C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup

To view either of these folders, you will need to enable the "View Hidden Files and Folders".

Registry

The Registry is a list of configurations, options and settings Windows computers use to operate. There are several folders here that an attacker can tell the computer to run a malicious file. The malicious file can be stored anywhere on the computer, and can be run from that location if told to do some from the registry.

Popular registry locations include:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

To check this, perform the following:

1. Press the Windows Key and the R key at the same time, and a new window should open up with a title of "Run"
2. In this window, type "regedit" and press enter
3. Now search through the directories listed above to the appropriate folder and review the contents in this folder.

Task Manager

The task scheduler is like an alarm clock for programs, and it launches different programs based on times and dates they are set to run on. I have seen this used for a few different reasons. The first reason is to schedule a malicious program to run every week/day/hour. The second is to have a sub program download and re-infect the computer every week/day//hour.

Imagine that you finish cleaning out the infections following this document, but skip this step. And imagine that there was a task scheduled to download the infection again and re-infect your computer. See the importance here?

To get to the Task Scheduler, follow the steps below.

1. Press the Windows Key and the R key at the same time, and a new window should open up called “Run”
2. Type “taskschd.msc” and press enter

Note that the Task Scheduler is visually divided into three sections. The Leftmost pane shows everything in a tree like structure. The middle pane describes the selected item and the rightmost pane acts as a context menu.

What you want to look for is:

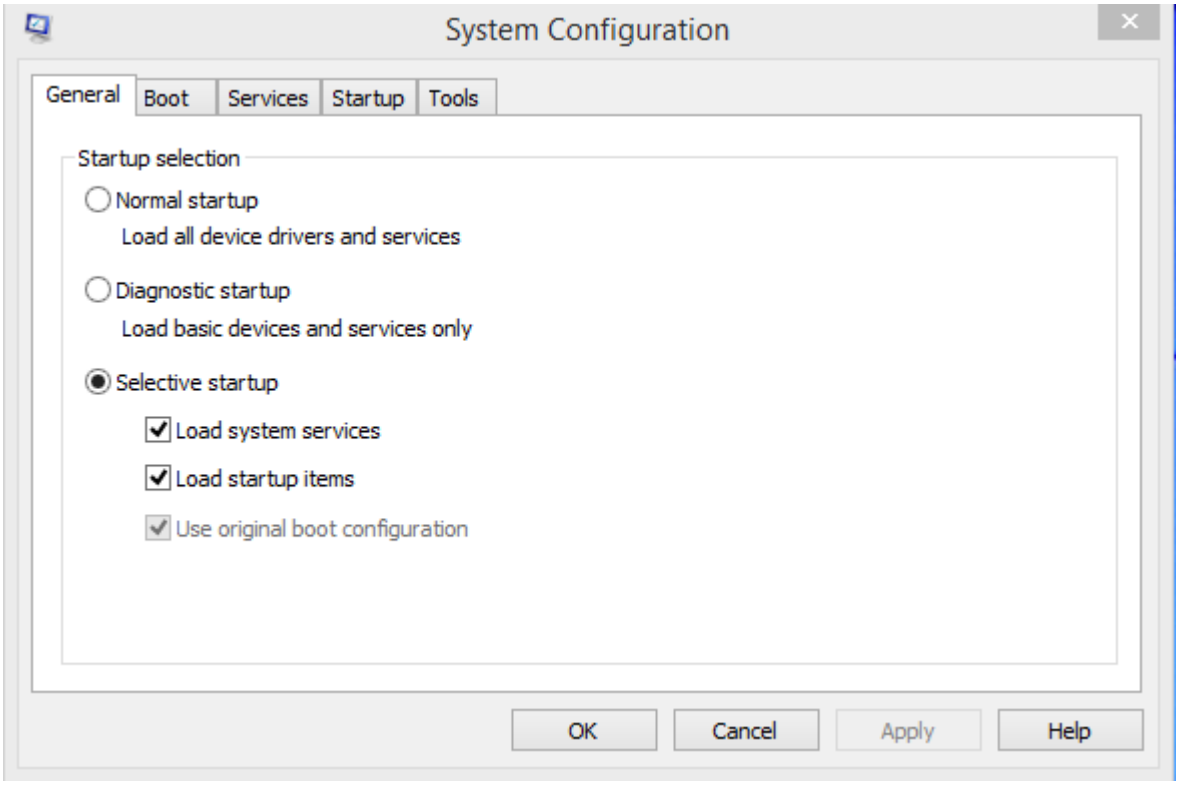
- random letters or words like 192837.exe or shredderhack.exe or 1.exe,
- Blank entries or no words or numbers

If you are familiar with Windows programs on your computer, then look for any programs that do not look familiar and disable them. If you discover you need them, then re-enable them. If you don’t need them, delete them.

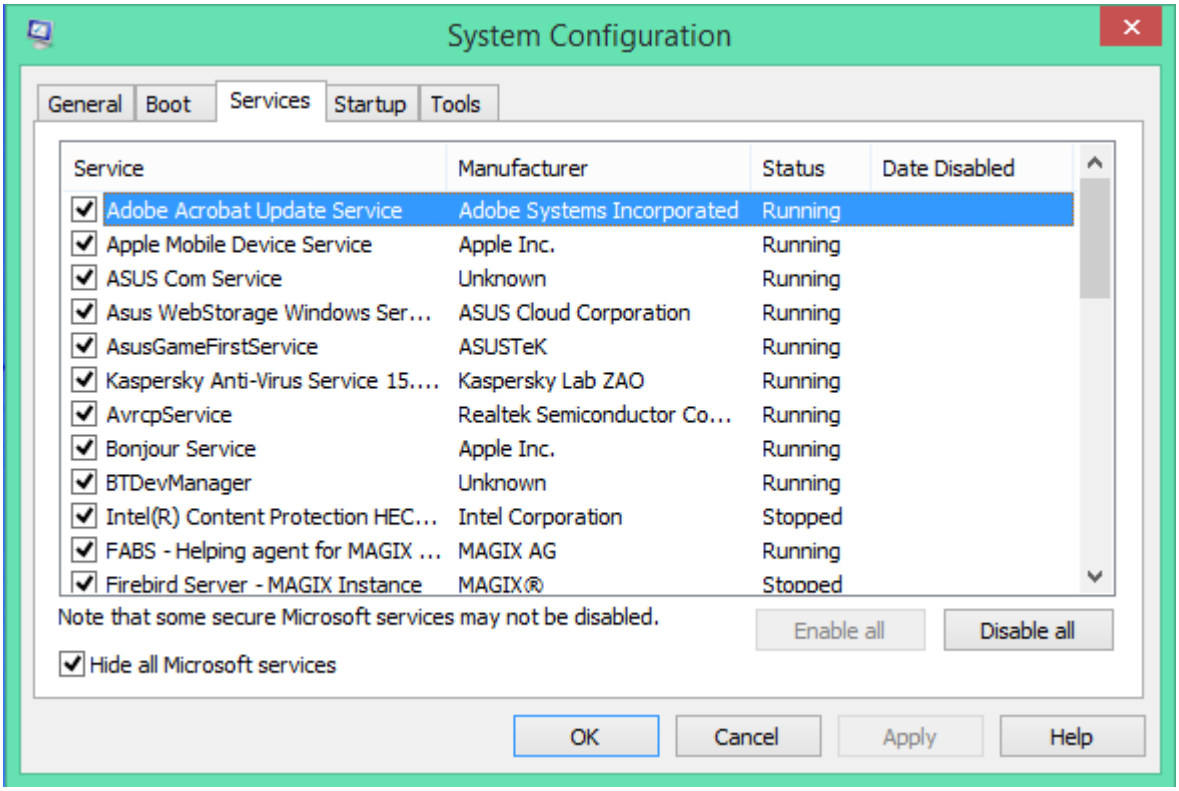
MSCONFIG

Microsoft built a tool that will help give you a snapshot of most of the information outlined above in a program called MSCONFIG. To access this program, do the following:

1. Press the Windows Key and the R key at the same time, and a new window should open up called “Run”
2. Type “MSCONFIG” and press enter



The System Configuration box will open and you have two options that you will want to pay attention to, Services and Startup.



In services, click on the option at the bottom called “Hide all Microsoft services” and review what is left over.

You are looking for the following:

- random letters or words like 192837.exe or shredderhack.exe or 1.exe,
- Blank entries or no words or numbers

If you see something you are not sure on, use your favorite search engine, and search for it. Read what others say about it. No matter what you find, I promise you that you are not the first to have it.

After this has been reviewed, look at the startup folder. Windows 7 shows some details, Windows 8 opens up Task Manager. This can help one identify things hidden in registry or the startup folders.

Conclusion

Now that you have looked at some startup locations, if you have found anything, it’s time to research it before going any further. Copy the file you found and search for it in your favorite search engine, and read the processes it takes to remove the program/infection.

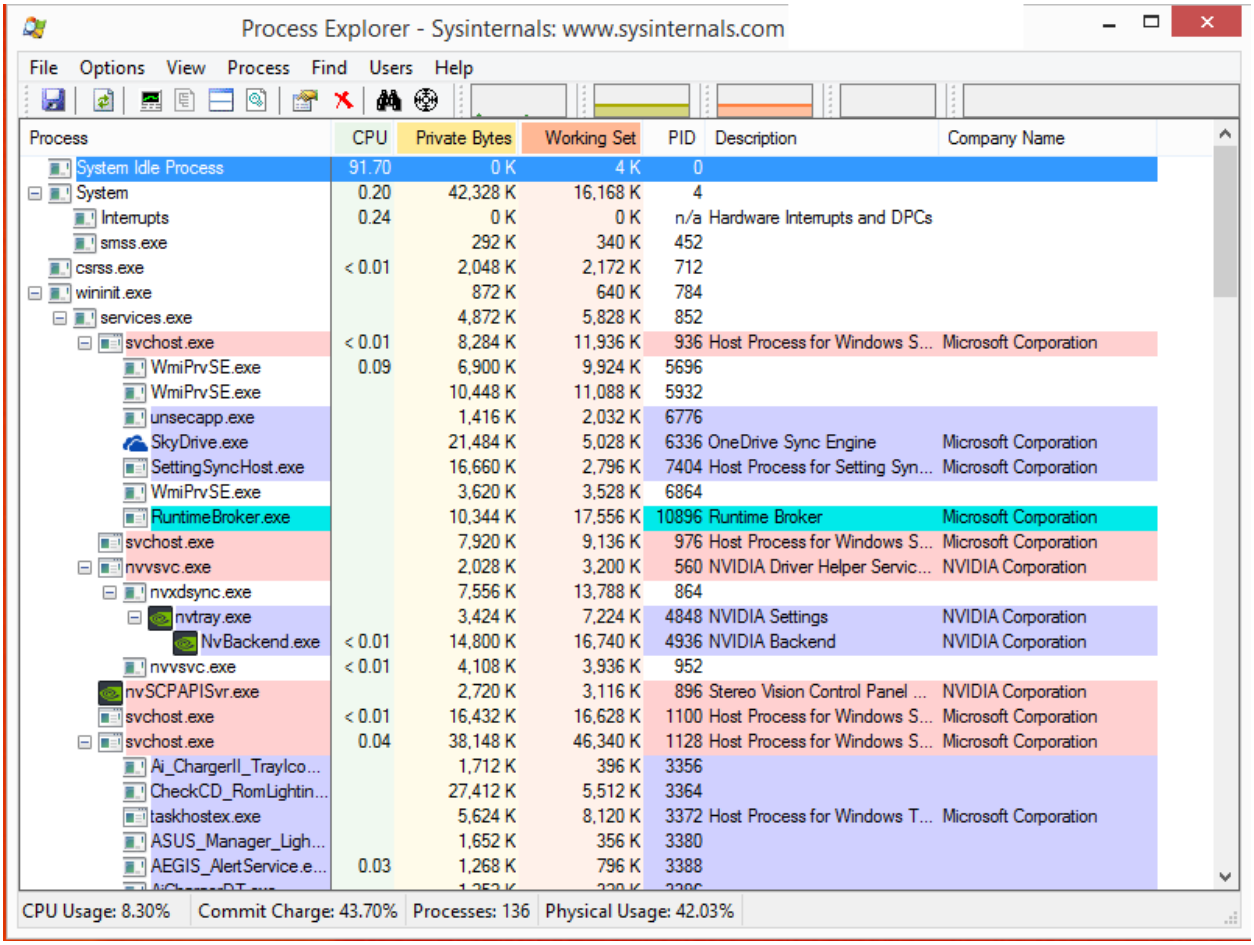
Step 2: Find the Infection

In this section, we actually attempt to find the infected files running or sitting in a directory on the computer. We use the following in this section:

- Process Explorer
- Windows File Explorer

Process Explorer

This is a free program available from Microsoft that will work on all versions of Windows. You can download it from technet.microsoft.com. Process Explorer[1] is designed to show you each program running on your computer, and what file or directory it is using or is located in. This is a very telling process to find anything running on your computer, and identify where it is, or it was run from. Once you run it and agree to the License Terms, you will be presented with a screen like below.



You will notice that there are colors, funny names you probably have not heard of, and lots of stuff. Don't panic, I will explain what you need to know for this exercise.

Colors:

[1] https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx

- Green = New Object
- Red = Deleted Objects
- Light Purple + Own Processes
- Peach = Services
- Grey = Suspended Processes
- Blue = Immersive Processes

Sections

- System Idle Process – Ignore this
- System – Ignore this
- CSRSS.exe – Ignore this
- Wininit.exe – Pay attention to the processes listed here.
- Winlogon.exe – Ignore this
- Explorer.exe – These are the programs that are running.

Key items to look for:

- Programs or processes that are running off of svchost.exe
- Processes that have no names
- Missing descriptions in the descriptions column
- Random letters and numbers as a process name

If you find a suspicious program running, there are a few things you can do to check for its legitimacy.

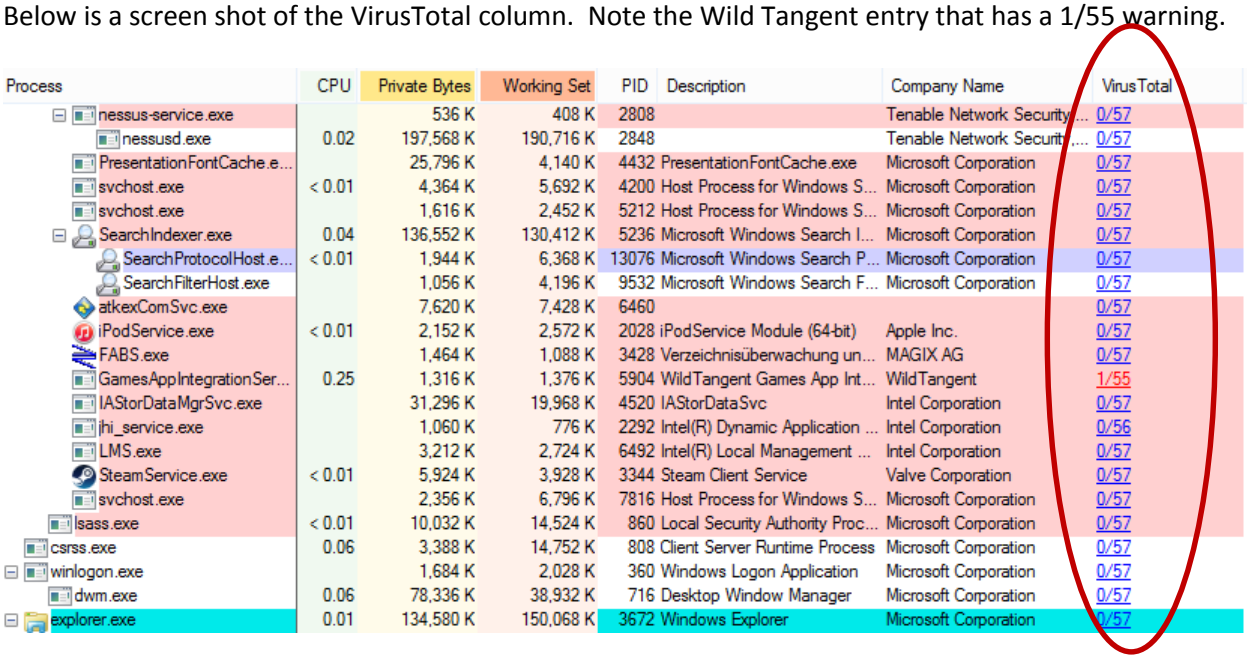
1. Right click on it and select Properties
    a. If its patch is not in Program Files or Program Files (32) or Windows/System32, research deeper.
    b. Look at its Autostart location, does its autostart name coincide with the name of the program? If they are vastly different, research deeper.
    c. Click on TCP/IP. Does it have entries here? If so, research deeper.
2. Right click on it and select "Check VirusTotal" and review the score it gets.
3. Right click on it and select "Research online" and read what others are saying about the file.

VirusTotal

Process Explorer comes with a free built in VirusTotal[2] checker. This is a quick way to identify something common and bad on your computer. What it does is take each executable and informs you if there is a concern/problem with it. It is important to note that it can raise concern about legit files, so don't panic if you see red. The higher the number the more concern you should have.

[2] https://www.virustotal.com/

Below is a screen shot of the VirusTotal column. Note the Wild Tangent entry that has a 1/55 warning.



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name	VirusTotal
nessus-service.exe		536 K	408 K	2808		Tenable Network Security,...	0/57
nessusd.exe	0.02	197,568 K	190,716 K	2848		Tenable Network Security,...	0/57
PresentationFontCache.e...		25,796 K	4,140 K	4432	PresentationFontCache.exe	Microsoft Corporation	0/57
svchost.exe	< 0.01	4,364 K	5,692 K	4200	Host Process for Windows S...	Microsoft Corporation	0/57
svchost.exe		1,616 K	2,452 K	5212	Host Process for Windows S...	Microsoft Corporation	0/57
SearchIndexer.exe	0.04	136,552 K	130,412 K	5236	Microsoft Windows Search I...	Microsoft Corporation	0/57
SearchProtocolHost.e...	< 0.01	1,944 K	6,368 K	13076	Microsoft Windows Search P...	Microsoft Corporation	0/57
SearchFilterHost.exe		1,056 K	4,196 K	9532	Microsoft Windows Search F...	Microsoft Corporation	0/57
atkexComSvc.exe		7,620 K	7,428 K	6460			0/57
iPodService.exe	< 0.01	2,152 K	2,572 K	2028	iPodService Module (64-bit)	Apple Inc.	0/57
FABS.exe		1,464 K	1,088 K	3428	Verzeichnisüberwachung un...	MAGIX AG	0/57
GamesAppIntegrationSer...	0.25	1,316 K	1,376 K	5904	WildTangent Games App Int...	WildTangent	1/55
IAStorDataMgrSvc.exe		31,296 K	19,968 K	4520	IAStorDataSvc	Intel Corporation	0/57
jhi_service.exe		1,060 K	776 K	2292	Intel(R) Dynamic Application ...	Intel Corporation	0/56
LMS.exe		3,212 K	2,724 K	6492	Intel(R) Local Management ...	Intel Corporation	0/57
SteamService.exe	< 0.01	5,924 K	3,928 K	3344	Steam Client Service	Valve Corporation	0/57
svchost.exe		2,356 K	6,796 K	7816	Host Process for Windows S...	Microsoft Corporation	0/57
lsass.exe	< 0.01	10,032 K	14,524 K	860	Local Security Authority Proc...	Microsoft Corporation	0/57
csrss.exe	0.06	3,388 K	14,752 K	808	Client Server Runtime Process	Microsoft Corporation	0/57
winlogon.exe		1,684 K	2,028 K	360	Windows Logon Application	Microsoft Corporation	0/57
dwm.exe	0.06	78,336 K	38,932 K	716	Desktop Window Manager	Microsoft Corporation	0/57
explorer.exe	0.01	134,580 K	150,068 K	3672	Windows Explorer	Microsoft Corporation	0/57

To use the VirusTotal feature, follow these steps:

1. Click on Options
2. Click on VirusTotal.com
3. Click on Check VirusTotal.com
4. Agree to the Terms
5. Review the VirusTotal score for each process running. Look for anything in red giving a score of 1 or higher out of 50+

Windows File Explorer

There are a few common areas that infections hang out in. These locations can be reviewed manually in Windows Explorer. Be sure to enable the show hidden files option.

Locations to pay close attention to:

- C:\Users\(user name)\AppData\local
- C:\Users\(user name)\AppData\local\temp
- C:\Users\(user name)\AppData\roaming

When I look at these directories, I sort the files and folders by date. First, there should be no .exe files in the root of these folders. If you see one, research it immediately. Even if it has a name you trust like skype.exe or aol.exe. These are most likely infections as legitimate programs do NOT place their executables here.

Next, look for names of programs you are not familiar with, and go in to each folder and look at what's inside. Any that you find, you will want to research. If any names are random letters and numbers, more than likely it's an infection.

Step 3: Remove the infection

Infections today are usually files stored on your system. Luckily, many infections are not creative and reside in some common areas of the computer system.

Registry

Remove any entries you may have found through the process above that are not supposed to be there. Be sure to back up your registry before removing. On rare occasions I have seen systems act sporadic after removing malicious entries because other files are looking for these entries. In which case, you can restore the registry and hunt down the cause of the issue.

Startup

Remove any startup items you may have found though the process above that are not supposed to be there.

Networking

Open up your network configurations for your wireless and wired adapter, and confirm the DNS and gateways are correct. If you never set this, there should be no entries in this and they should be cleared. I have seen once, where a system was compromised to use an attackers DNS server remotely. This was discovered due to local networking issues and domain issues with this workstation.

Browser

If you are investigating how an infection got on the system, the browser history files are critical. Once you have made copies or have reviewed them, delete them. Delete everything and reset the browser to default settings. Please note at this time, there has been no declared safe browser. So regardless if you use IE, Chrome or Firefox, you need to do this.

I would also recommend checking any add-ons in the browser. This process is outside the scope of this paper, but a simple search engine search will lead you to simple steps to follow for your browser of preference.

Temp Folders

Empty these. It is filled with things you do not need and is safe to delete everything you can. Note that there will be some files in there you will not be able to delete, just skip those. After you have emptied these folders, empty the trash.

C:\Windows\Temp
C:\Users\(user name)\AppData\Local\Temp

AppData Folders

This is where I find most infections hiding out in. These folders exist for every user on the computer. If you share your computer with someone else, you will need to do this for each user.

These folders contain certain information for certain programs. Generally speaking, there should be no files at the root other than a .db file and perhaps a log. If you see any .exe or .bat or other executable type of file, there is a good chance it's up to no good. Please note that some programs do store EXE here, but I have never seen a need for them.

> "There was one case I saw skype.exe and aol.exe here. Both were malicious programs disguised to trick the user in to trusting them. The real version of these programs is usually stored in program files, not here."

After you have reviewed and removed files at the root of these folders, it is time to review the folders. Malicious programs may also create folders here and store their needed files in them. If you see a suspicious folder, open it and look at the contents. Again, if there are .exe of .bat or any other executable file type, consider these as malicious. Feel free to cut these folders to a temporary folder somewhere else of your choosing, and restart your computer. Check to see if there are any errors or prompts that come up complaining about missing files or folders. If not, delete those files/folders you just moved to the temp folder.

Here are the concerned folders:

> C:\Users\(user name)\AppData\Local
> C:\Users\(user name)\AppData\Roaming

Tools

Malwarebytes[3] is a tool I use to double check myself. It will give me a confirmation that I didn't miss anything obvious and I always run it after I perform my analysis. I do this because I want to know the infection and impact, and a tool like this could remove some of the infection, but perhaps not all of it. It may also misreport the infection thinking it's one thing when in fact it was just a small part of something bigger.

When you run Malwarebytes, be sure to read the report, understand what you may have missed, and learn from it. Chances are the next few infections out there will have a similar file and install pattern.

[3] https://www.malwarebytes.org/

Step 4: If All Else Fails

If after you have done all of this, and are pulling your hair out because popups, or whatever nuisances are still plaguing you, your best line is to rebuild your computer from scratch. I recall listening to Stephen Northcut once talk about how interesting it is that in the Windows world, we can add all we want to a computer, but to remove it is another game. One that is not easy, takes time and knowledge. Since I tend to look at time as money, sometimes the quickest fix is to start over, and guarantee results.

Step 5: Lessons Learned

Now that you have identified an infection, and cleaned it out, you have a better understanding of how it got there, and what the weak point was. Here is a list taken from SANS top 20 Critical Security Controls[4] that apply to every user:

- Malware Defenses – Have Antivirus installed, updated and checking every night
- Data Recovery Capability – Be sure to have backups that do not reside on the computer
- Controlled use of administrative privileges – NEVER run as an administrator. There is no need today, run-as will be your best friend.
- Secure configurations for hardware and software – Patch your system as soon as patches are released for both, the OS and the software you have installed

Conclusion

I hope this paper gives you a little more knowledge, perhaps the desire to research more, learn more. There are many approaches out there, spend the time to research them, read up on them, and come to your own conclusion on how to address infections. As I mentioned, if you come across something on your computer, there is a really good chance you are not the first. Use your favorite search engine to learn more about it.

[4] http://www.sans.org/critical-security-controls/